8. How do you analyze and interpret scan results in Nessus?

📊 Analyzing and Interpreting Nessus Scan Results

Once a Nessus scan is completed, analyzing the results effectively is crucial for identifying vulnerabilities and taking corrective actions. This guide will walk you through **how to view, interpret, and prioritize Nessus scan results** to strengthen your security posture. 🚀

📌 1. Accessing Scan Results in Nessus

After running a scan, follow these steps to **view and analyze the results**:

1️⃣ **Log in to Nessus** (`https://localhost:8834`)
2️⃣ Click on **"Scans"** in the left menu
3️⃣ Locate the completed scan and click on it
4️⃣ The **Scan Results** page will display vulnerabilities, severity levels, and affected assets

✅ **Pro Tip:** Click on **"History"** to see previous scan results and compare changes over time.

📊 2. Understanding Nessus Scan Results

Nessus provides a **detailed breakdown** of vulnerabilities, categorized by severity levels and affected systems. The results are displayed in the **Scan Summary**.

🖥️ A. Key Sections of Scan Results

Section	Description
Hosts	Lists all scanned devices and their vulnerabilities
Vulnerabilities	Shows detected vulnerabilities with severity levels
Plugins	Details on specific vulnerabilities and exploitability
Compliance	Checks for policy violations and misconfigurations
Remediation	Recommended fixes for identified vulnerabilities

✅ **Best Practice:** Focus on **high and critical severity** vulnerabilities first, as they pose the most risk.

🚦 3. Interpreting Vulnerability Severity Levels

Nessus uses **CVSS (Common Vulnerability Scoring System)** to rank vulnerabilities by severity:

Severity	CVSS Score	Description
🔴 **Critical**	9.0 - 10.0	Severe risk; immediate exploitation possible
🟠 **High**	7.0 - 8.9	Exploitable vulnerability with high impact
🟡 **Medium**	4.0 - 6.9	Possible exploitation but requires effort
🔵 **Low**	0.1 - 3.9	Low risk but should still be addressed
⚪ **Info**	N/A	General information about system security

✅ **Prioritization Tip:**

- **Critical (🔴) & High (🟠) vulnerabilities** should be **patched ASAP**.
- **Medium (🟡) vulnerabilities** should be addressed **in a timely manner**.
- **Low (🔵) & Info (⚪) issues** may not require immediate action but should be reviewed.

🔎 4. Analyzing Detailed Vulnerability Information

Each vulnerability in Nessus contains **detailed descriptions** to help you understand its impact.

🔍 How to View Details of a Vulnerability

1️⃣ Click on a **vulnerability name** in the scan results
2️⃣ The **vulnerability details page** will open
3️⃣ Review the following key fields:

Field	Description
Description	Explains what the vulnerability is
CVE ID	Links to public vulnerability databases (e.g., CVE-2024-xxxx)
Exploitability	Indicates if the vulnerability is actively exploited
Affected Hosts	Shows which systems are vulnerable
Risk Factor	Critical, High, Medium, Low, or Info
Solution	Recommended fix or mitigation

✅ **Pro Tip:** If a vulnerability has a **known exploit**, prioritize fixing it to prevent attacks.

🛠️ 5. Using Filters to Prioritize Vulnerabilities

Nessus allows you to **filter vulnerabilities** based on different criteria.

🎯 How to Filter Results for Better Analysis

1️⃣ Click **"Vulnerabilities"** in the scan results
2️⃣ Use the **Filters** section to refine your search
3️⃣ Apply filters like:

- **Severity** (Show only Critical & High vulnerabilities)
- **Exploitability** (Show only vulnerabilities with known exploits)
- **Affected Hosts** (Focus on high-value targets like web servers)
  4️⃣ Review the filtered list and prioritize accordingly

✅ **Best Practice:** Export filtered reports for quick review by security teams.

📢 6. Understanding Compliance & Configuration Findings

If your scan includes **compliance checks**, Nessus will flag security misconfigurations.

🔎 What to Look For?

- **Weak Password Policies** (e.g., no complexity requirements)
- **Unpatched Software** (e.g., outdated SSH, RDP, or web services)
- **Missing Security Controls** (e.g., firewall disabled, unnecessary open ports)

✅ **Fixing Compliance Issues** helps meet industry standards like **PCI-DSS, HIPAA, and NIST**.

📂 7. Exporting Nessus Scan Reports

You can export results in different formats for further analysis.

📤 How to Export a Nessus Scan Report

1️⃣ Open the **Scan Results**
2️⃣ Click on **"Export"** in the top-right corner
3️⃣ Choose a format:

- **PDF** → Easy to read, good for management reports
- **CSV** → For further analysis in Excel
- **Nessus XML** → For importing into another Nessus instance
  4️⃣ Click **"Download"**

✅ **Pro Tip:** Use **CSV exports** for filtering vulnerabilities in **Excel or SIEM tools**.

🚀 8. Taking Action: Remediation & Mitigation

Once you've analyzed vulnerabilities, the next step is **fixing them**.

🛠️ Best Practices for Vulnerability Remediation

✓ **Patch Management** – Apply updates for OS, software, and services
✓ **Configuration Hardening** – Disable unnecessary services & tighten security settings
✓ **Network Segmentation** – Limit exposure by isolating critical systems
✓ **Firewall & IPS Rules** – Block exploitation attempts with security controls
✓ **Re-Scan After Fixes** – Verify vulnerabilities are patched

✅ **Pro Tip:** Use Nessus to schedule **follow-up scans** to confirm fixes are applied.

🔚 Final Thoughts

Mastering Nessus scan results helps you **detect, prioritize, and fix vulnerabilities efficiently**. By understanding severity levels, using filters, and following best practices for remediation, you can **reduce security risks and improve system defenses**.